

#4
DB
7-20-01

PATENT
81942.0012

Express Mail Label No. EL 713 623 649 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Daisuke SUZUKI et al.

Serial No: Not assigned

Filed: January 24, 2001

For: ENCRYPTION METHOD, DECRYPTION
METHOD, CRYPTOGRAPHIC
COMMUNICATION SYSTEM AND
ENCRYPTION DEVICE

Art Unit: Not assigned

Examiner: Not assigned



TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

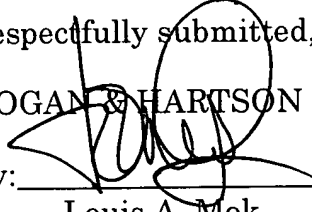
Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-14704 which was filed May 18, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,
HOGAN & HARTSON L.L.P.

Date: January 25, 2001

By: 
Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

Jc974 U.S. PTO
09/771021
01/25/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 5月18日

出 願 番 号

Application Number:

特願2000-147047

出 願 人

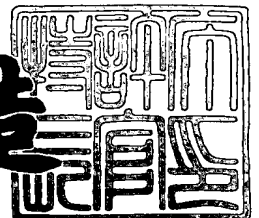
Applicant (s):

村田機械株式会社
境 隆一
笠原 正雄

2000年 8月18日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3064849

【書類名】 特許願

【整理番号】 20992

【特記事項】 特許法第 3 0 条第 1 項の規定の適用を受けようとする特
許出願

【提出日】 平成12年 5月18日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 暗号化方法，復号方法，暗号通信システム，暗号化装置
及び記録媒体

【請求項の数】 10

【発明者】

 【住所又は居所】 大阪府豊能郡豊能町東ときわ台 9 - 3 - 1 1

 【氏名】 鈴木 大祐

【発明者】

 【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株
式会社 本社工場内

 【氏名】 村上 恭通

【発明者】

 【住所又は居所】 京都府京都市山科区安朱東海道町 1 6 - 2 緑山荘 B
棟 1 0 1 号室

 【氏名】 境 隆一

【発明者】

 【住所又は居所】 大阪府箕面市粟生外院 4 丁目 1 5 番 3 号

 【氏名】 笠原 正雄

【特許出願人】

 【識別番号】 000006297

 【氏名又は名称】 村田機械株式会社

 【代表者】 村田 純一

【特許出願人】

【識別番号】 599100556

【氏名又は名称】 境 隆一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化方法、復号方法、暗号通信システム、暗号化装置及び記録媒体

【特許請求の範囲】

【請求項 1】 暗号化すべき平文を分割した平文ベクトルと公開鍵ベクトルとを用いて積和型の暗号文を得る暗号化方法において、前記平文ベクトルに所定の変換を施して変換ベクトルを生成し、前記平文ベクトル及び前記変換ベクトルの成分と前記公開鍵ベクトルの成分とによる積和演算により暗号文を得ることを特徴とする暗号化方法。

【請求項 2】 前記平文ベクトルの各成分と前記変換ベクトルの各成分とを交互に用いて前記公開鍵ベクトルの成分との積和演算を行う請求項 1 記載の暗号化方法。

【請求項 3】 前記公開鍵ベクトルは基数積ベクトルを基にモジュラ変換したものである請求項 1 または 2 記載の暗号化方法。

【請求項 4】 前記平文ベクトル及び前記変換ベクトルの成分は (m_1, m_2, \dots, m_K) と示され、前記公開鍵ベクトルの成分は基数積ベクトル (B_1, B_2, \dots, B_K) (但し、基数 b_i ($1 \leq i \leq K$) を用いて $B_i = b_1 b_2 \dots b_i$) の成分 B_i をモジュラ変換したものであり、前記基数 b_i として、 m_i が前記変換ベクトルの成分である場合には $b_i > m_{i-1}$ を満たす正規基数を用い、 m_i が前記平文ベクトルの成分である場合には $b_i \leq m_{i-1}$ を満たす退化基数を用いる請求項 1 または 2 記載の暗号化方法。

【請求項 5】 平文に基づく第 1 ベクトルと基数積をモジュラ変換した成分からなる第 2 ベクトルとを用いて積和型の暗号文を得る暗号化方法において、暗号化すべき平文を分割した平文ベクトルと該平文ベクトルを所定の関数を用いて変換した変換ベクトルとにて前記第 1 ベクトルを構成し、 $b_i > m_{i-1}$ (b_i は前記基数積における基数、 m_{i-1} は前記第 1 ベクトルの成分、 $2 \leq i \leq K$ (K は前記第 1, 第 2 ベクトルの成分数)) を満たす正規基数と $b_j \leq m_{j-1}$ (b_j は前記基数積における基数、 m_{j-1} は前記第 1 ベクトルの成分、 $2 \leq j \leq K$) を満たす退化基数とにて前記基数積を構成することを特徴とする暗号化方法。

【請求項 6】 請求項 1～4 の何れかに記載の暗号化方法にて得られる暗号文を復号する方法であって、復号した前記平文ベクトルの成分に基づいて前記変換ベクトルを復号することを特徴とする復号方法。

【請求項 7】 請求項 4 または 5 に記載の暗号化方法にて得られる暗号文を復号する方法であって、復号された正規基数の部分に基づいて退化基数の部分を復号することを特徴とする復号方法。

【請求項 8】 複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項 1～5 の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項 9】 平文から積和型の暗号文を得る暗号化装置において、暗号化すべき平文を分割して平文ベクトルを得る手段と、前記平文ベクトルに所定の変換を施して変換ベクトルを生成する手段と、前記平文ベクトル及び前記変換ベクトルの成分と公開鍵ベクトルの成分とによる積和演算により暗号文を得る手段とを備えることを特徴とする暗号化装置。

【請求項 10】 コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割して平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記平文ベクトルに所定の変換を施して変換ベクトルを生成することをコンピュータに実行させるプログラムコード手段と、前記平文ベクトル及び前記変換ベクトルの成分と公開鍵ベクトルの成分とによる積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、平文を積和型の暗号文に変換するための暗号化方法、及び、積和型の暗号文を平文に変換するための復号方法、並びに、これらを用いた暗号通信シ

システム、暗号化装置及びこの暗号化方法の動作プログラムを記録した記録媒体に関する。

【 0 0 0 2 】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュートリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【 0 0 0 3 】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【 0 0 0 4 】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【 0 0 0 5 】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異っており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【0006】

【発明が解決しようとする課題】

公開鍵暗号系の1つである、整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、多進法を用いることにより、高速な復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特願平10-262036号）。

【0007】

この暗号化方法及び復号方法における処理は、以下のように行う。暗号化すべき平文を K 分割して平文ベクトル $m = (m_1, m_2, \dots, m_K)$ を得る。また、基数 b_i ($1 \leq i \leq K$) による基数積と、乱数 v_i とを用いて $B_i = v_i b_1 b_2 \dots b_i$ を設定する。 P を素数とし、乱数 w とこの B_i とを用いて公開鍵 c_i は $c_i \equiv w B_i \pmod{P}$ により計算される。ここで、 c_i は公開鍵、 b_i , v_i , P , w は秘密鍵である。送信者は、公開鍵 c_i を用いて暗号文 $C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K$ による暗号化を行う。受信者は、中間復号文 $M \equiv w^{-1} C \pmod{P}$ を求め、逐次復号アルゴリズムにより復号を行う。このようにして、平文を多進法を用いて表現するようにしたので、高速な復号を行うことができる。

【0008】

また、LLL (Lenstra-Lenstra-Lovasz) 法を用いた低密度攻撃に対して強くすることを目的として、上記暗号化方法の改良方法を本発明者等は提案している（特願平11-173338号、以下先行例という）。この先行例は、誤り訂正符号を用いた退化積和型暗号方式であり、上記暗号化方法及び復号方法に以下のような要

素を付加したものである。

1. 暗号化すべき各分割平文を誤り訂正符号化したものを上記 m_i とする。
2. 基数 $\{b_i\}$ のうち、特定の位置以降には適当な個数の退化基数を用い、その他は正規基数を用いる。但し、退化基数、正規基数は夫々 $m_{i-1} \geq b_i$, $m_{i-1} < b_i$ を満たす基数である。
3. 退化基数の影響によって復号できない m_i に関しては、誤り訂正符号の能力を用いて復号する。

【0 0 0 9】

先行例では、最も前に配置された退化基数の前までの m_i を解読できることが判明した。そこで、最初の退化基数をできる限り前に配置することが考えられるが、このようにした場合には、大きな誤り訂正能力が必要であって実用的でないという問題点がある。

【0 0 1 0】

このような退化基数を用いる手法は、平文に冗長性を持たせて密度（入力平文長／暗号文長）を大きくでき、LLL法に基づく攻撃に対する耐性の向上を期待できる有効な手法であり、本発明者等は、このような退化積和型暗号方式の更なる手法を研究している。

【0 0 1 1】

本発明は斯かる事情に鑑みてなされたものであり、先行例の問題点を解決できて、LLL法に基づく攻撃に対して強く、高速に暗号化及び復号を行える暗号化方法及び復号方法、並びに、これらを用いた暗号通信システム、暗号化装置及びこの暗号化方法の動作プログラムを記録した記録媒体を提供することを目的とする。

【0 0 1 2】

【課題を解決するための手段】

請求項1に係る暗号化方法は、暗号化すべき平文を分割した平文ベクトルと公開鍵ベクトルとを用いて積和型の暗号文を得る暗号化方法において、前記平文ベクトルに所定の変換を施して変換ベクトルを生成し、前記平文ベクトル及び前記変換ベクトルの成分と前記公開鍵ベクトルの成分とによる積和演算により暗号文

を得ることを特徴とする。

【0013】

請求項2に係る暗号化方法は、請求項1において、前記平文ベクトルの各成分と前記変換ベクトルの各成分とを交互に用いて前記公開鍵ベクトルの成分との積和演算を行うことを特徴とする。

【0014】

請求項3に係る暗号化方法は、請求項1または2において、前記公開鍵ベクトルは基数積ベクトルを基にモジュラ変換したものであることを特徴とする。

【0015】

請求項4に係る暗号化方法は、請求項1または2において、前記平文ベクトル及び前記変換ベクトルの成分は (m_1, m_2, \dots, m_K) と示され、前記公開鍵ベクトルの成分は基数積ベクトル (B_1, B_2, \dots, B_K) (但し、基数 b_i ($1 \leq i \leq K$) を用いて $B_i = b_1 b_2 \dots b_i$) の成分 B_i をモジュラ変換したものであり、前記基数 b_i として、 m_i が前記変換ベクトルの成分である場合には $b_i > m_{i-1}$ を満たす正規基数を用い、 m_i が前記平文ベクトルの成分である場合には $b_i \leq m_{i-1}$ を満たす退化基数を用いることを特徴とする。

【0016】

請求項5に係る暗号化方法は、平文に基づく第1ベクトルと基数積をモジュラ変換した成分からなる第2ベクトルとを用いて積和型の暗号文を得る暗号化方法において、暗号化すべき平文を分割した平文ベクトルと該平文ベクトルを所定の関数を用いて変換した変換ベクトルとにて前記第1ベクトルを構成し、 $b_i > m_{i-1}$ (b_i は前記基数積における基数、 m_{i-1} は前記第1ベクトルの成分、 $2 \leq i \leq K$ (K は前記第1, 第2ベクトルの成分数)) を満たす正規基数と $b_j \leq m_{j-1}$ (b_j は前記基数積における基数、 m_{j-1} は前記第1ベクトルの成分、 $2 \leq j \leq K$) を満たす退化基数とにて前記基数積を構成することを特徴とする。

【0017】

請求項6に係る復号方法は、請求項1～4の何れかに記載の暗号化方法にて得られる暗号文を復号する方法であって、復号した前記平文ベクトルの成分に基づいて前記変換ベクトルを復号することを特徴とする。

【 0 0 1 8 】

請求項 7 に係る復号方法は、請求項 4 または 5 に記載の暗号化方法にて得られる暗号文を復号する方法であって、復号された正規基数の部分に基づいて退化基数の部分で復号することを特徴とする。

【 0 0 1 9 】

請求項 8 に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項 1 ～ 5 の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備えることを特徴とする。

【 0 0 2 0 】

請求項 9 に係る暗号化装置は、平文から積和型の暗号文を得る暗号化装置において、暗号化すべき平文を分割して平文ベクトルを得る手段と、前記平文ベクトルに所定の変換を施して変換ベクトルを生成する手段と、前記平文ベクトル及び前記変換ベクトルの成分と公開鍵ベクトルの成分とによる積和演算により暗号文を得る手段とを備えることを特徴とする。

【 0 0 2 1 】

請求項 1 0 に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割して平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記平文ベクトルに所定の変換を施して変換ベクトルを生成することをコンピュータに実行させるプログラムコード手段と、前記平文ベクトル及び前記変換ベクトルの成分と公開鍵ベクトルの成分とによる積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする。

【 0 0 2 2 】

誤り訂正符号を用いた退化積和型暗号方式である先行例では、それまでの積和型暗号方式と比べて高密度であるので、LLL法に基づく攻撃に強いと考えられていたが、解読されることが判明した。この解読の原因は、退化基数を連続的に

末尾に配置したことによる。従って、LLL法に基づく攻撃に強くするためには、退化基数を比較的前方に配置することが有効であると考えられる。但し、先行例では退化基数を前方に配置した場合、誤り訂正能力を大きくしなければならなかった。

【0023】

本発明では、平文の拡大変換を用いた退化積和型暗号方式を提案する。本発明では、誤り訂正符号とは異なる拡大変換という新たな手法を導入する。暗号化すべき平文ベクトルに所定の変換を施して密度向上のための変換ベクトルを生成して、平文の拡大変換を行う。そして、平文ベクトル及び変換ベクトルの成分と公開鍵ベクトルの成分とによる積和演算により暗号文を得る。暗号文の復号時に、通常の復号が適用できない退化部分を、上記所定の変換に応じて再生する。

【0024】

本発明では、平文の拡大変換という手法により、より多くの退化基数を配置することが可能となる。よって、積和型暗号の特徴である暗号化・復号の高速性を維持しながら、密度を容易に大きく設定できてLLL法に基づく攻撃に強い。また、誤り訂正符号のような複雑な暗号化／復号処理が必要ではなく、簡単に暗号化／復号処理を行える。

【0025】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、退化積和型暗号方式を採用した本発明における暗号化方法をエンティティa、b間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティa側で、平文Xを暗号文Cに暗号化し、通信路1を介してその暗号文Cを他方のエンティティbへ送信し、エンティティb側で、その暗号文Cを元の平文Xに復号する場合を示している。

【0026】

送信側のエンティティaには、平文Xを複数の分割平文に分割して複数のメッセージ $m_1, m_3, \dots, m_{2j-1}, \dots$ を得る平文分割器2と、これらの奇数番目のメッセージ $m_1, m_3, \dots, m_{2j-1}, \dots$ から密度を向上させるためのダミーメッセー

ジ $m_2, m_4, \dots, m_{2j}, \dots$ を生成するダミーメッセージ生成器 3 と、これらのメッセージ $m_1, m_2, m_3, m_4, \dots, m_{2j-1}, m_{2j}, \dots, m_K$ と公開鍵 c_1, c_2, \dots, c_K とを用いて暗号文 C を作成する暗号化器 4 とが備えられている。一方、受信側のエンティティ b には、後述する分岐逐次復号アルゴリズムに従って各メッセージ m_i ($1 \leq i \leq K$) を求めて、送られてきた暗号文 C を元の平文 X に復号する復号器 5 が備えられている。

【 0 0 2 7 】

次に、具体的な手法について説明する。

〔準備〕

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵： $\{b_i\}, \{v_i\}, P, w$
- ・公開鍵： $\{c_i\}, f(\cdot)$

【 0 0 2 8 】

各メッセージ m_i の大きさを e ビットとする。即ち、各メッセージ m_i は下記 (1) を満たす。

$$m_i < 2^e \quad \dots (1)$$

【 0 0 2 9 】

まず、平文 X を分割して、奇数番目のメッセージ $m_1, m_3, \dots, m_{2j-1}, \dots$ を得る。次に、メッセージ生成関数 $f(\cdot)$ を用いて、奇数番目のメッセージ m_{2j-1} から偶数番目のメッセージ m_{2j} を生成することにより、平文の拡大変換を行う。ここで、偶数番目のメッセージは密度を向上させるためのダミーメッセージであり、全メッセージの総数を K とした場合、真に有効なメッセージの数は下記 (2) となる。

【 0 0 3 0 】

【数 1】

$$\left\lfloor \frac{K+1}{2} \right\rfloor \dots (2)$$

【0031】

また、基数 b_i は下記 (3) を満たす整数とする。

【0032】

【数2】

$$b_i = \begin{cases} 2^e + \delta_i & (1 \ll \delta_i \ll 2^e) \\ & (i=2j) \\ 2^{e'} + \delta'_i & (1 \ll \delta'_i \ll 2^{e'}, e' < e) \\ & (i=2j-1) \end{cases} \cdots (3)$$

【0033】

基数積 $b_1 b_2 \cdots b_i$ に乱数 v_i を乗じて、基数ベクトル $B = (B_1, B_2, \dots, B_K)$ を下記 (4) のように設定する。

$$B_i = v_i b_1 b_2 \cdots b_i \quad \cdots (4)$$

【0034】

ここで、上記 (4) で示される各成分 B_i がほぼ同じ大きさになるように乱数 v_i を設定する。但し、 $\gcd(v_i, b_{i+1}) = 1$ を満たすものとする。

【0035】

乱数 w を用いて、公開鍵 c_i は下記 (5) のモジュラ変換により求められる。

$$c_i \equiv w B_i \pmod{P} \quad \cdots (5)$$

【0036】

〔暗号化〕

暗号文 C は、各メッセージ m_i と公開鍵 c_i とを用いた積和演算によって与えられる。暗号文 C は、具体的には下記 (6) のように表される。

$$C = m_1 c_1 + m_2 c_2 + \cdots + m_K c_K \quad \cdots (6)$$

【0037】

〔復号〕

以下のようにして復号処理が行われる。暗号文 C に対して、中間復号文 M を下記 (7) のようにして求める。

$$M \equiv w^{-1}C \pmod{P} \quad \dots (7)$$

【0038】

そして、下記(8)に示す分岐逐次復号アルゴリズムに従って、各メッセージ m_i の復号を行う。

【0039】

【数3】

[分岐逐次復号アルゴリズム]

ステップ1

$$M_1 = \frac{M}{b_1}$$

$$m_1 \equiv M_1 v_1^{-1} \pmod{b_2}$$

ステップ i ($2 \leq i \leq K-1$)

$$M_i = \frac{M_{i-1} - m_{i-1} v_{i-1}}{b_i}$$

$$m_i = \begin{cases} M_i v_i^{-1} \pmod{b_{i+1}} & (i=2j-1) \\ f(m_{i-1}) & (i=2j) \end{cases} \quad (8)$$

ステップK

Kが偶数の場合

処理なし

Kが奇数の場合

$$M_K = \frac{M_{K-1} - m_{K-1} v_{K-1}}{b_K}$$

$$m_K = M_K v_K^{-1}$$

【0040】

このアルゴリズムにあつては、奇数番目のメッセージ m_i については従来と同様の手法にて復号し、偶数番目のメッセージ m_i についてはメッセージ生成関数 $f(\cdot)$ を用いて $m_i = f(m_{i-1})$ により復号する。

【0041】

ここで、メッセージ生成関数 $f(\cdot)$ について考察する。本発明の暗号化方式がLLL法に基づく攻撃に高い耐性を有するためには、 $f(\cdot)$ が線形であってはならない。例えば、 $f(\cdot)$ が恒等変換である場合、即ち $m_{2j} = m_{2j-1}$ である場合には、暗号文Cを下記(9)のように変形できるので、下記(10)に示すようにして公開鍵を下記(11)の個数に変換し、低密度攻撃を適用すれば、平文を求めることが可能である。

【0042】

【数4】

$$\begin{aligned} C &= m_1 c_1 + m_2 c_2 + \dots + m_K c_K \\ &= m_1 (c_1 + c_2) + \dots + m_{K-1} (c_{K-1} + c_K) \dots (9) \end{aligned}$$

$$c'_i = c_{2i-1} + c_{2i} \left(i \leq \left\lfloor \frac{K+1}{2} \right\rfloor \right) \dots (10)$$

$$\left\lfloor \frac{K+1}{2} \right\rfloor \dots (11)$$

【0043】

また、 $f(\cdot)$ が非線形である場合でも、必ずしも安全である保証はない。例えば、 $f(x) = ax + b$ (具体的に、 $f(\cdot)$ がメッセージ m_i の各ビットを反転するものであるときには $a = -1$, $b = 2^e - 1$) とした場合、暗号文Cを下記(12)のように変形できるので、下記(13), (14)に示すようになることにより、公開鍵を下記(15)の個数に変換し、同様に低密度攻撃を適用すれば、平文を求めることが可能である。

【0044】

【数5】

$$C = m_1 (c_1 + a c_2) + \dots + b (c_2 + c_4 + \dots + c_K) \quad \dots (12)$$

$$C' = C - b \sum_{j=1}^{\lfloor (K+1)/2 \rfloor} c_{2j} \quad \dots (13)$$

$$c_t' = c_{2t+1} + a c_{2t+2} \quad \dots (14)$$

$$\left\lfloor \frac{K+1}{2} \right\rfloor \quad \dots (15)$$

【0045】

安全と考えられるメッセージ生成関数 $f(\cdot)$ としては、下記 (16), (17) 等を一例として挙げる事ができる。但し、 q は e ビットの素数、 u は e ビットの整数とする。

【0046】

【数6】

$$f(x) = x^2 \bmod q \quad \dots (16)$$

$$f(x) = x \oplus u \quad \dots (17)$$

(\oplus は各ビットの排他的論理和演算)

【0047】

このメッセージ生成関数 $f(\cdot)$ は、信頼できるセンタが公開しても良いし、エンティティが公開するようにしても良い。この $f(\cdot)$ におけるビット演算は整数環上での非線形な変換であるので、上記 (17) のような論理演算を導入した場合、センタが公開した u をパラメータとする $f(\cdot)$ に対し、エンティティは u のみを公開する方法も可能である。

【0048】

次に、本発明の暗号化方式における暗号化レートと密度とについて考察する。退化積和型暗号における暗号化レート r は、平文長／暗号文長で定義される。また、密度 ρ は退化積和型暗号への入力文長／暗号文長で定義され、本発明の方式では密度 ρ は拡大平文長／暗号文長である。ここで、平文長 L_p ，拡大平文長 L_E ，暗号文長 L_C は夫々下記 (18)，(19)，(20) のようになる。よって、暗号化レート r ，密度 ρ は夫々下記 (21)，(22) のようになる。

【0049】

【数 7】

$$L_p = \left\lfloor \frac{K+1}{2} \right\rfloor e \cdots (18)$$

$$L_E = K e \cdots (19)$$

$$L_C \geq \begin{cases} e + \log_2 K + \frac{K e}{2} + \frac{(K-2) e'}{2} & (K: \text{偶数}) \\ e + \log_2 K + \frac{(K-1) e}{2} + \frac{(K-1) e'}{2} & (K: \text{奇数}) \end{cases} \cdots (20)$$

$$r \leq \frac{L_p}{L_C} \doteq \frac{e}{e + e' + (\log_2 K)/K} \cdots (21)$$

$$\rho = \frac{L_E}{L_C} \cdots (22)$$

【0050】

本発明の暗号化方式にあって、 e' / e の値、即ち退化基数のビットサイズ e' を小さくした場合に、暗号化レート r は大きくなり、密度 ρ も向上する。従って、退化基数サイズを小さくすることにより、LLL法に基づく攻撃に対して高

い耐性を有することができる。

【 0 0 5 1 】

本発明の暗号化方式では、上記 (20) , (22) より、最小ブロック数 $K = 3$ である場合でも密度 ρ は 1 を超え、LLL 法に基づく攻撃に対して高い耐性を有することを期待できる。この場合、 $e = 64$, $e' / e = \alpha$ としたときに、暗号文長 L_C は下記 (23) の条件を満たすことができ、従来の公開鍵暗号と比較して、ブロックサイズが非常に小さい画期的な暗号方式を設計できる。

$$L_C = 128 + 1.6 + 64\alpha < 194 \quad \cdots (23)$$

【 0 0 5 2 】

図 2 は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、上述した例において、暗号化すべき平文を分割して奇数番目のメッセージを得る処理、メッセージ生成関数 $f(\cdot)$ を用いて奇数番目のメッセージから偶数番目のメッセージを生成する処理、及び、これらのメッセージと公開鍵とを用いて積和型の暗号文を作成する処理を含んでいるか、または、上述した分岐逐次復号アルゴリズムに従って暗号文を元の平文に復号する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ 20 は、送信側または受信側のエンティティに設けられている。

【 0 0 5 3 】

図 2 において、コンピュータ 20 とオンライン接続する記録媒体 21 は、コンピュータ 20 の設置場所から隔たって設置される例えば WWW (World Wide Web) のサーバコンピュータを用いてなり、記録媒体 21 には前述の如きプログラム 21 a が記録されている。記録媒体 21 から読み出されたプログラム 21 a がコンピュータ 20 を制御することにより、コンピュータ 20 が、平文から暗号文を作成するか、または、暗号文を平文に復号する。

【 0 0 5 4 】

コンピュータ 20 の内部に設けられた記録媒体 22 は、内蔵設置される例えばハードディスクドライブまたは ROM などを用いてなり、記録媒体 22 には前述の如きプログラム 22 a が記録されている。記録媒体 22 から読み出されたプログラム 22 a がコンピュータ 20 を制御することにより、コンピュータ 20 が、

平文から暗号文を作成するか、または、暗号文を平文に復号する。

【 0 0 5 5 】

コンピュータ 2 0 に設けられたディスクドライブ 2 0 a に装填して使用される記録媒体 2 3 は、運搬可能な例えば光磁気ディスク、CD-ROM またはフレキシブルディスクなどを用いてなり、記録媒体 2 3 には前述の如きプログラム 2 3 a が記録されている。記録媒体 2 3 から読み出されたプログラム 2 3 a がコンピュータ 2 0 を制御することにより、コンピュータ 2 0 が、平文から暗号文を作成するか、または、暗号文を平文に復号する。

【 0 0 5 6 】

なお、上述した例では、暗号通信システムの場合について説明したが、平文を暗号化して暗号文を作成し、作成した暗号文を単に記録するような場合にも、本発明の暗号化方法を適用できることは勿論である。

【 0 0 5 7 】

【発明の効果】

以上のように、本発明では、平文の拡大変換を用いて暗号化するようにしたので、先行例に比べて、LLL 法に基づく攻撃に対する耐性を向上できる。また、誤り訂正符号を用いた先行例のように複雑な暗号化／復号処理を必要とせず、暗号化／復号時の演算処理を少なくでき、簡単かつ高速に暗号化／復号処理を行える。また、暗号ブロック数の低減も図れるので、小規模なハードウェアにより暗号通信システムを構築できる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図 1】

2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 2】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

- 1 通信路
- 2 平文分割器

3 ダミーメッセージ生成器

4 暗号化器

5 復号器

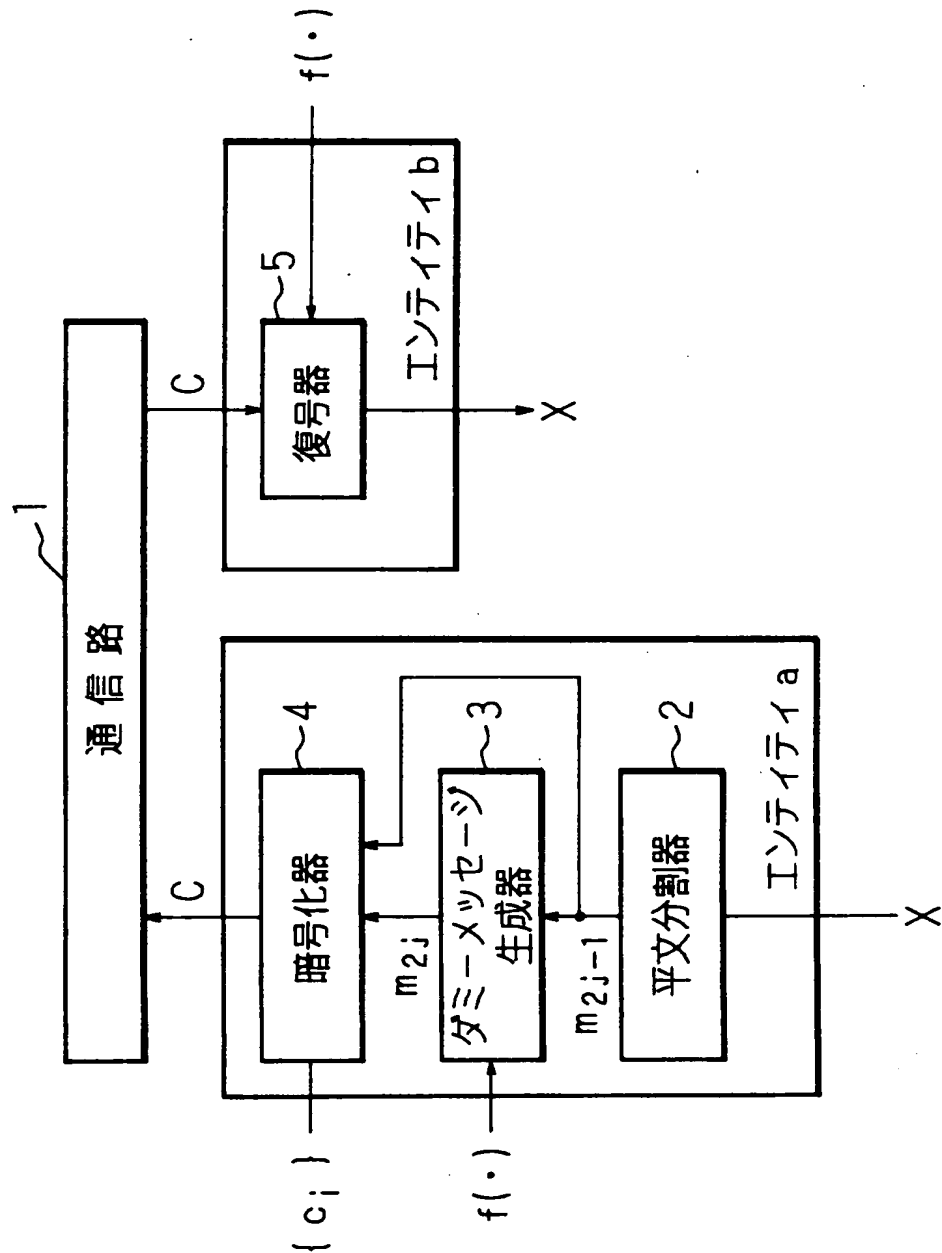
2 0 コンピュータ

2 1, 2 2, 2 3 記録媒体

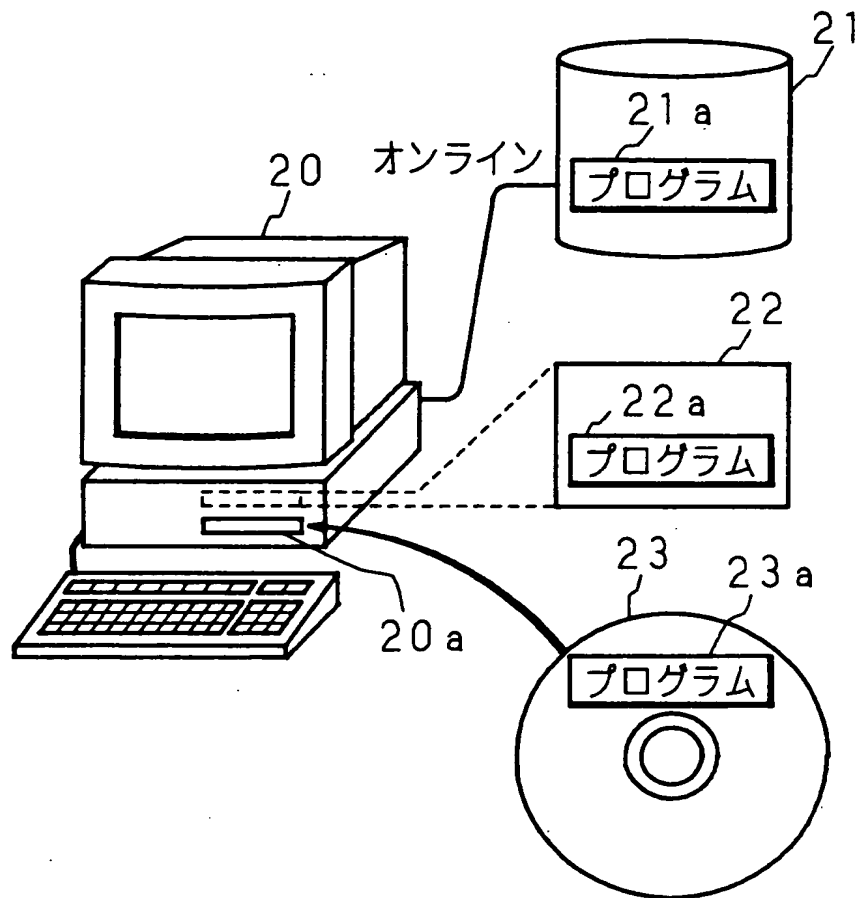
a, b エンティティ

【書類名】 図面

【図 1】



【図 2】



【書類名】 要約書

【要約】

【課題】 LLL法に基づく攻撃に対する耐性が高く、しかも簡単な演算処理にて暗号化／復号を高速に行える暗号化／復号方法を提供する。

【解決手段】 平文を拡大変換した後に、退化積和型の暗号化を行う。暗号化すべき平文を分割して平文ベクトルを得、その平文ベクトルを関数 $f(\cdot)$ にて変換して変換ベクトルを生成し、平文ベクトル及び変換ベクトルをメッセージとして公開鍵 c_i (基数積ベクトル) との積和演算にて暗号文 C を作成する。

【選択図】 図1

認定・付加情報

| | |
|---------|---------------|
| 特許出願の番号 | 特願2000-147047 |
| 受付番号 | 50000616157 |
| 書類名 | 特許願 |
| 担当官 | 第七担当上席 0096 |
| 作成日 | 平成12年 6月30日 |

<認定情報・付加情報>

【特許出願人】

| | |
|----------|--------------------|
| 【識別番号】 | 000006297 |
| 【住所又は居所】 | 京都府京都市南区吉祥院南落合町3番地 |
| 【氏名又は名称】 | 村田機械株式会社 |

【特許出願人】

| | |
|----------|---------------------|
| 【識別番号】 | 599100556 |
| 【住所又は居所】 | 京都府京都市山科区安朱東海道町16-2 |
| 【氏名又は名称】 | 境 隆一 |

【特許出願人】

| | |
|----------|--------------------|
| 【識別番号】 | 597008636 |
| 【住所又は居所】 | 大阪府箕面市栗生外院4丁目15番3号 |
| 【氏名又は名称】 | 笠原 正雄 |

【代理人】

| | |
|----------|---------------------------------|
| 【識別番号】 | 100078868 |
| 【住所又は居所】 | 大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所 |
| 【氏名又は名称】 | 河野 登夫 |

【選任した復代理人】

| | |
|----------|---------------------------------|
| 【識別番号】 | 100114557 |
| 【住所又は居所】 | 大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所 |
| 【氏名又は名称】 | 河野 英仁 |

出 願 人 履 歴 情 報

識別番号 [000006297]

| | |
|----------|--------------------|
| 1. 変更年月日 | 1990年 8月 7日 |
| [変更理由] | 新規登録 |
| 住 所 | 京都府京都市南区吉祥院南落合町3番地 |
| 氏 名 | 村田機械株式会社 |

出 願 人 履 歴 情 報

識別番号 [599100556]

1. 変更年月日 1999年 7月16日
[変更理由] 新規登録
住 所 京都府京都市山科区四ノ宮柳山町8
氏 名 境 隆一
2. 変更年月日 2000年 6月14日
[変更理由] 住所変更
住 所 京都府京都市山科区安朱東海道町16-2
氏 名 境 隆一

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日 1997年 1月21日

[変更理由] 新規登録

住 所 大阪府箕面市粟生外院4丁目15番3号

氏 名 笠原 正雄